NOTICE OF DATA BREACH

January 21, 2022

You are receiving this Notice because you are a current or former employee of Custom Personnel, Inc., Diversified Resource Management, Inc., PEI Ohio, Inc., Premium Enterprises, Inc., Premium of Indiana, Inc., Premium of North Carolina, Inc., Premium of Tennessee, Inc., or Custom Payroll Services, Ltd. (each, a "Premium Company"). **Please read this important notice.**

What Happened

On January 2, 2022, the Premium Companies received a ransom demand from an unknown person (the "Hacker") claiming that the Hacker had gained access to employee personal information. We believe the Hacker breached the Premium Companies' website's employer portal between December 29, 2021 and January 2, 2022 and accessed roughly 20% of the Premium Companies' files related to current and former employees. The Hacker posted some employee information on a public website.

What Information Was Involved

The employee personal information accessed by the Hacker may include names, addresses, telephone numbers, email addresses, social security numbers, dates of birth, and driver's license numbers. We have confirmed that the Hacker accessed only a portion of the Premium Companies' employee files, but we are not able to identify the specific files the Hacker accessed.

What We Are Doing

We engaged an outside IT expert to conduct an investigation and to implement additional safeguards including temporarily shutting down our website and removing employer access to all employee personal information from our website. Currently, the website has been reinstated, but any employee information is only accessible to a restricted group of our IT personnel, and we are continuing to explore additional security measures. We also changed passwords and implemented two-factor authentication on our internal system.

What You Can Do

Please see the attached "Information about Identity Theft Prevention" for steps you can take to avoid fraud and identity theft. Because we cannot positively identify the files the Hacker accessed, we recommend that you consider taking all of the identified precautions, including obtaining a copy of your credit reports, implementing a credit freeze, and placing a fraud alert on your credit reports.

For More Information

In the event you have any questions about this event and how it may affect you, please call 330-722-7974 Ext 600. We will continue to work to make our systems and your information more secure. The Premium Companies take employee security and this event very seriously and regret that it may have affected you in any way.

Information about Identity Theft Prevention

It is recommended that you remain vigilant for any incidents of fraud or identity theft by regularly reviewing credit card account statements, financial statements, and your credit report for unauthorized activity. You may obtain a free copy of your credit report every twelve months from the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281, 1-877-322-8228, or by accessing the website at www.annualcreditreport.com.

You can obtain information from the consumer reporting agencies, the **Federal Trade Commission (FTC)**, or your state Attorney General about steps you can take to prevent identity theft. You may report suspected identity theft to local law enforcement, the FTC, or your Attorney General. The FTC may be contacted at 1-877-438-4338, or at www.identitytheft.gov.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national consumer reporting agencies listed below.

Equifax: 1- 800-685-1111, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1- 888-909-8872, www.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting agency. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting agency*. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major consumer reporting agencies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348,
https://www.equifax.com/personal/credit-report-services/credit-freeze/
Experian: Experian Security Freeze, P.O. Box 9554, Allen, TX 75013,
https://www.experian.com/freeze/center.html
TransUnion: P.O. Box 2000, Chester, PA, 19016,
https://www.transunion.com/credit-freeze

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national consumer reporting agencies listed above.